THE TECHNOLOGY PROVIDER

FORTIOS 7.2 NEUE FEATURES

Andreas Tischer, Fortinet
Martin Ruesch, ALSO Schweiz AG
Chris Tanasic, ALSO Schweiz AG

21. Juni 2022

WILLKOMMEN BEI TECH & SNACK, TEIL 2 ☺

WER WIR SIND

Andreas (Andi) Tischer

Channel PreSales Engineer
Fortinet

Martin (Tinu) Ruesch

Tech. Consultant Security
ALSO Schweiz

Cvijetin (Chris) Tanasic

Tech. Consultant Security
ALSO Schweiz

AGENDA

- **Was gibt es Neues?**
  - **Neue FortiGate Releases**
  - **FortiCare – Was ist neu?**
- **Topic: FortiOS 7.2 – Neue Features inkl. Demo**
- **Q & A**

HOUSEKEEPING RULES

Das Webinar wird aufgezeichnet!

MS Teams Chat für Fragen verwenden

Slides werden nachträglich verschickt

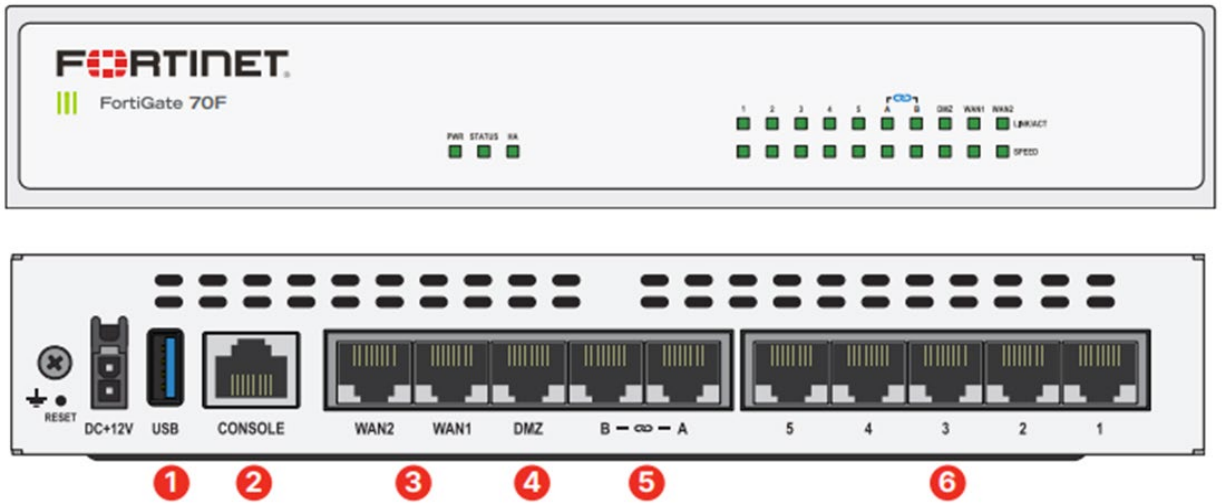
Fragebogen/Survey ausfüllen

MUESLI-BECHER VON MYMUESLI.CH

FORTIGATE – NEUE MODELLE

FORTIGATE 70F

FortiGate 70F/ 71F



Interfaces

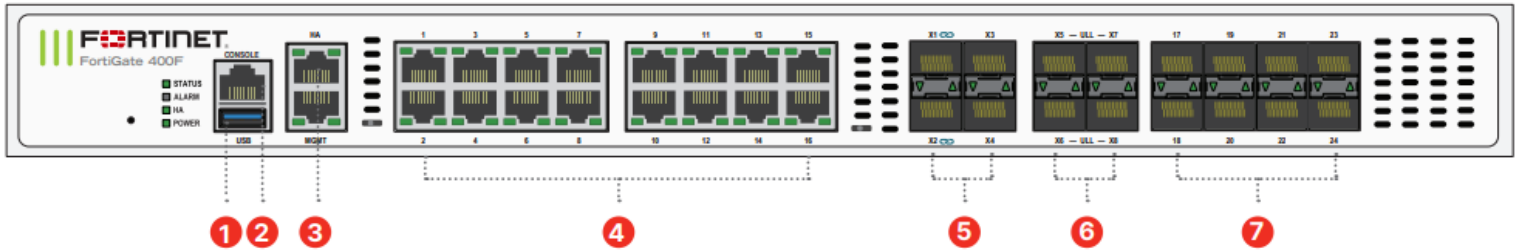
1. 1x USB Port
2. 1x Console Port
3. 2x GE RJ45 WAN Ports
4. 1x GE RJ45 DMZ Port
5. 2x GE RJ45 FortiLink Ports
6. 5x GE RJ45 Internal Ports

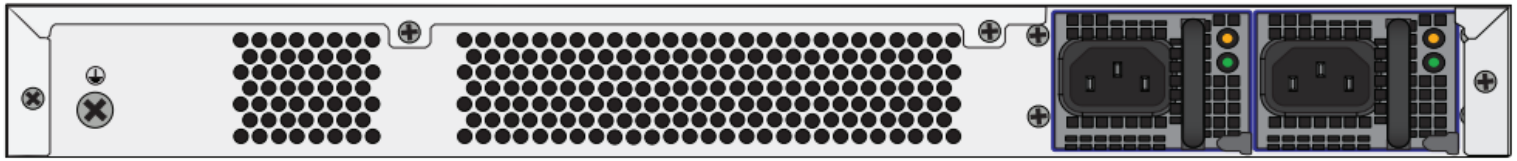
Hardware Features

Firewall	IPS	NGFW	Threat Protection*
10 Gbps	1.4 Gbps	1 Gbps	800 Mbps

FORTIGATE 400F

FortiGate 400F/401F

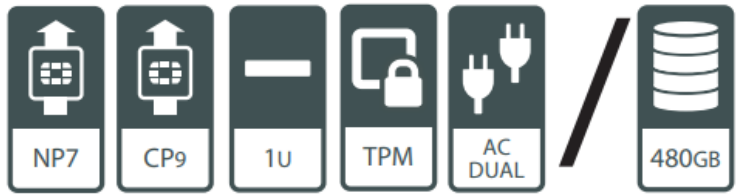




Interfaces

1. 1x USB Port
2. 1x Console Port
3. 2x GE RJ45 MGMT/HA Ports
4. 16x GE RJ45 Ports
5. 4× 1GE/10GE SFP+ Slots
6. 4× 10GE SFP+ Ultra Low Latency Slots
7. 8× 1GE SFP Slots

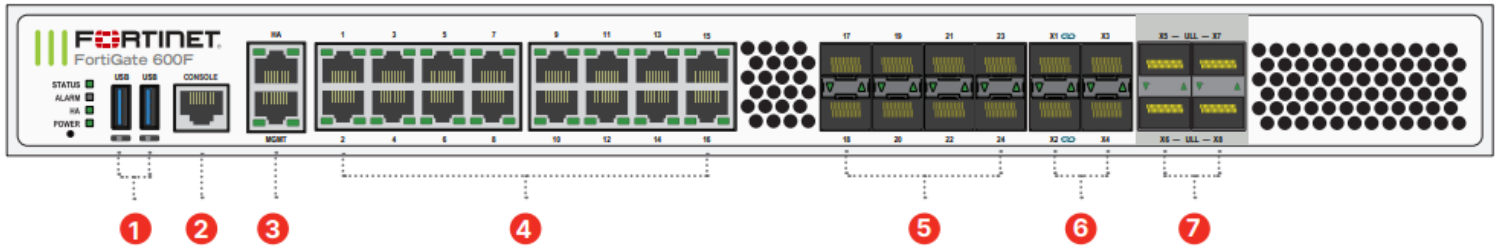
Hardware Features

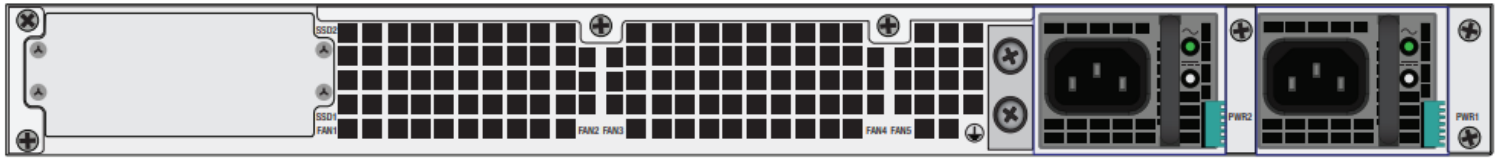


Firewall*	IPS*	NGFW*	Threat Protection*
80 Gbps	10 Gbps	8 Gbps	6 Gbps

FORTIGATE 600F

FortiGate 600F/601F

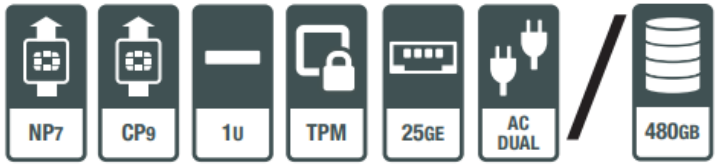




Interfaces

1. 2x USB Ports
2. 1x Console Port
3. 2x GE RJ45 MGMT/HA Ports
4. 16x GE RJ45 Ports
5. 8x GE SFP Slots
6. 4× 10GE/GE SFP+/SFP Slots
7. 4× 25GE/10GE SFP28/SFP+ Ultra Low Latency Slots

Hardware Features



Firewall*	IPS*	NGFW*	Threat Protection*
140 Gbps	12 Gbps	9 Gbps	8 Gbps

FORTICARE – NEUE SUPPORT-STUFEN

FORTICARE – NEUE SUPPORT-STUFEN

- **FortiCare Essential**
  - Neuestes, billigeres FortiCare für tiefere FortiGate-Modelle (bis 80-Serie)
  - Support beinhaltet lediglich WEB ONLY TICKETS und Chat, sowie Next-Business-Day-Response
  - Kein Telefon-Support!
- **FortiCare Premium**
  - Bisheriges 24x7 FortiCare mit FTS-Support, sowie 1h-Reaktion
  - Service-Spektrum bleibt gleich
- **FortiCare Elite**
  - Bisheriges ASE FortiCare mit FTS-Support, sowie 15min-Reaktion
  - Breiteres Service-Spektrum
  - Auch für FAP, FS, FAZ, FMG

FORTIOS 7.2 – NEUE FEATURES

PLATFORM SUPPORT - FORTIOS 7.2.0

= zu einem späteren Zeitpunkt verfügbar, möglicherweise bei Patch-Veröffentlichungen

Grau = EoO-Produkte

	6.4.9	7.0.6	7.2
FG/FWF-60E	●	●	●
FG/FWF-40F Series	●	●	●
FG/FWF-60F Series	●	●	●
FG-80E Series	●	●	●
FG/FWF-80F Series	●	●	●
FG-90E Series	●	●	●
FG-100/101E Series	●	●	●
FG-100F Series	●	●	●
FG-200/201E	●	●	●
FG-200F	●	●	●
FG-300E/500E Series	●	●	●
FG-400E/600E Series	●	●	●
FG-800D/900D/1x00D Series	●	●	●

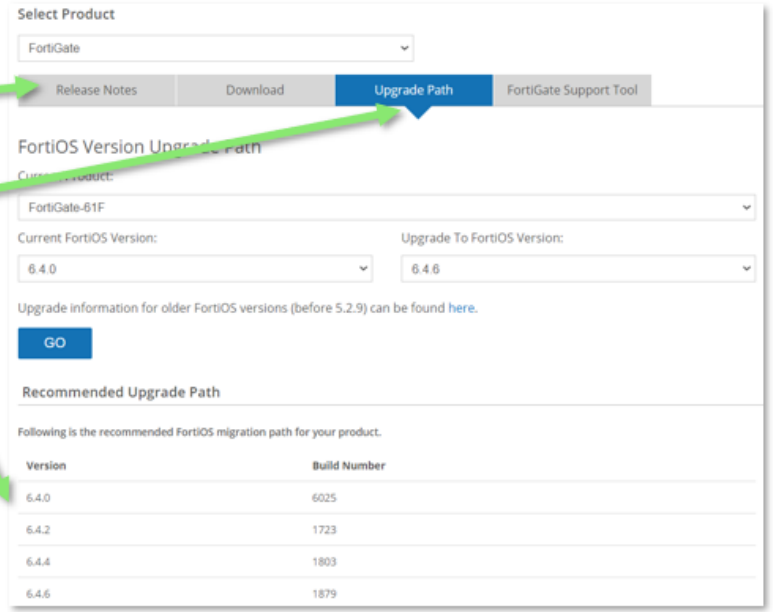
	6.4.9	7.0.6	7.2
FG-1100E Series	●	●	●
FG-1800F Series	●	#	#
FG-2200E, 3300E Series	●	●	●
FG-2000E, 2500E	●	●	●
FG-2600F Series	●	#	#
FG-3X00D Series (inc. 3800D)	●	●	●
FG-3810/3815D	●		
FG-3400E/3600E	●	●	●
FG-3500F series	●	#	#
FG-3960E/3980E	●	●	●
FG-4200/4400F Series	●	#	#
FG-5001D	●		
FG-5001E	●	●	●
FG-6000/7000 Series	●	#	#

DAS WISSEN WIR EIGENTLICH.... UPGRADEN

FORTIGATE UPGRADEN – VORBEREITUNG

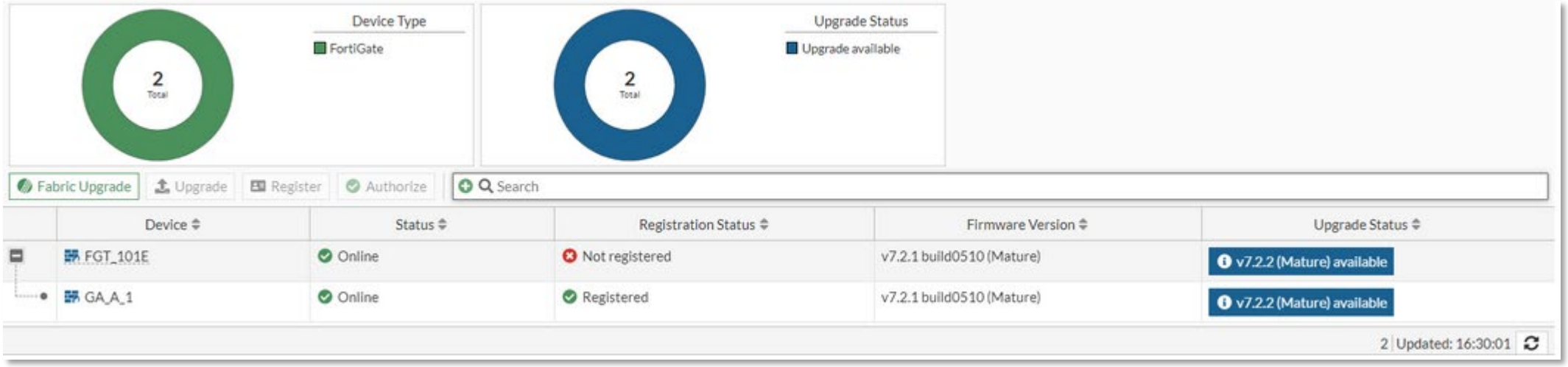
FortiOS 6.4

- Software kann über das Supportportal von Fortinet heruntergeladen werden
- Release Notes durchlesen
- Upgrade Pfad unbedingt beachten
- Backup der Konfiguration erstellen
- Die FortiGate startet nach dem Upgrade neu

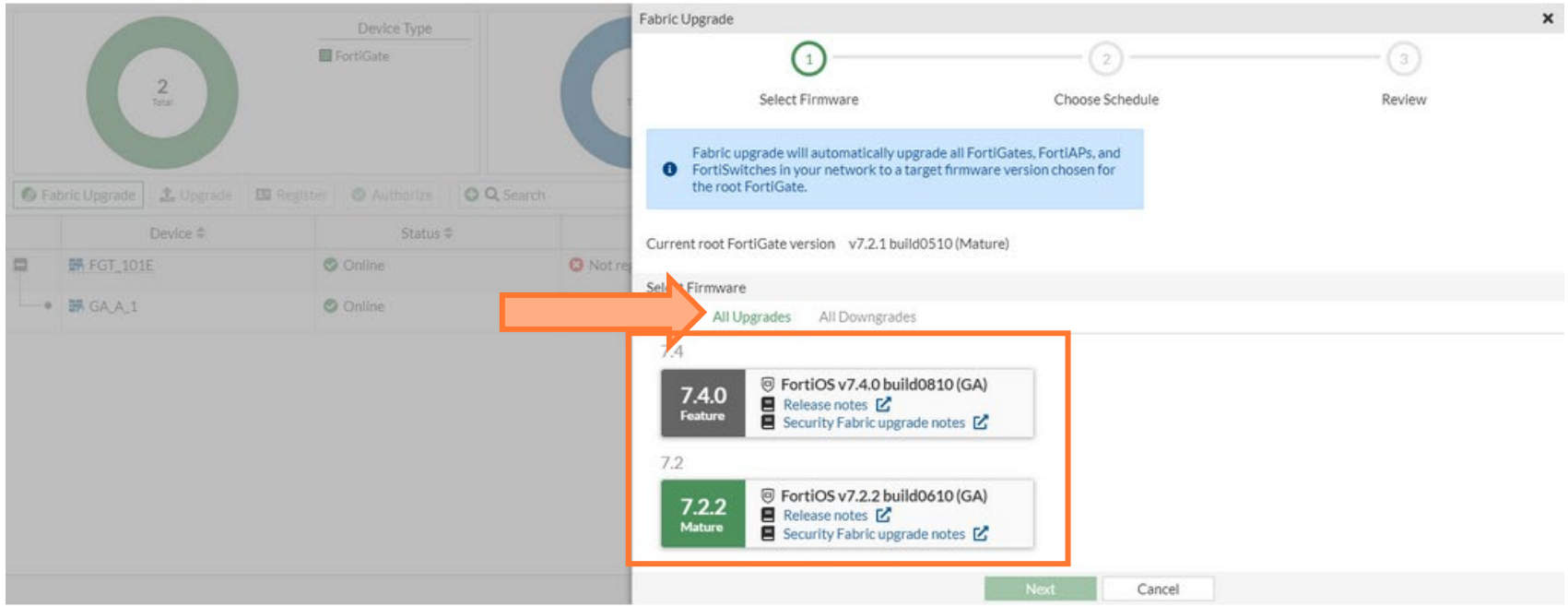


FOLLOW UPGRADE PATH

- Neue Option: Follow Upgrade path
  - Die Ziel-Firmware wird gemäss Upgrade-Path installiert, so dass Administratoren alle Upgrades einfach nacheinander durchführen können (mit mehreren Neustarts)
  - kann sofort oder zu einem geplanten Zeitpunkt durchgeführt werden

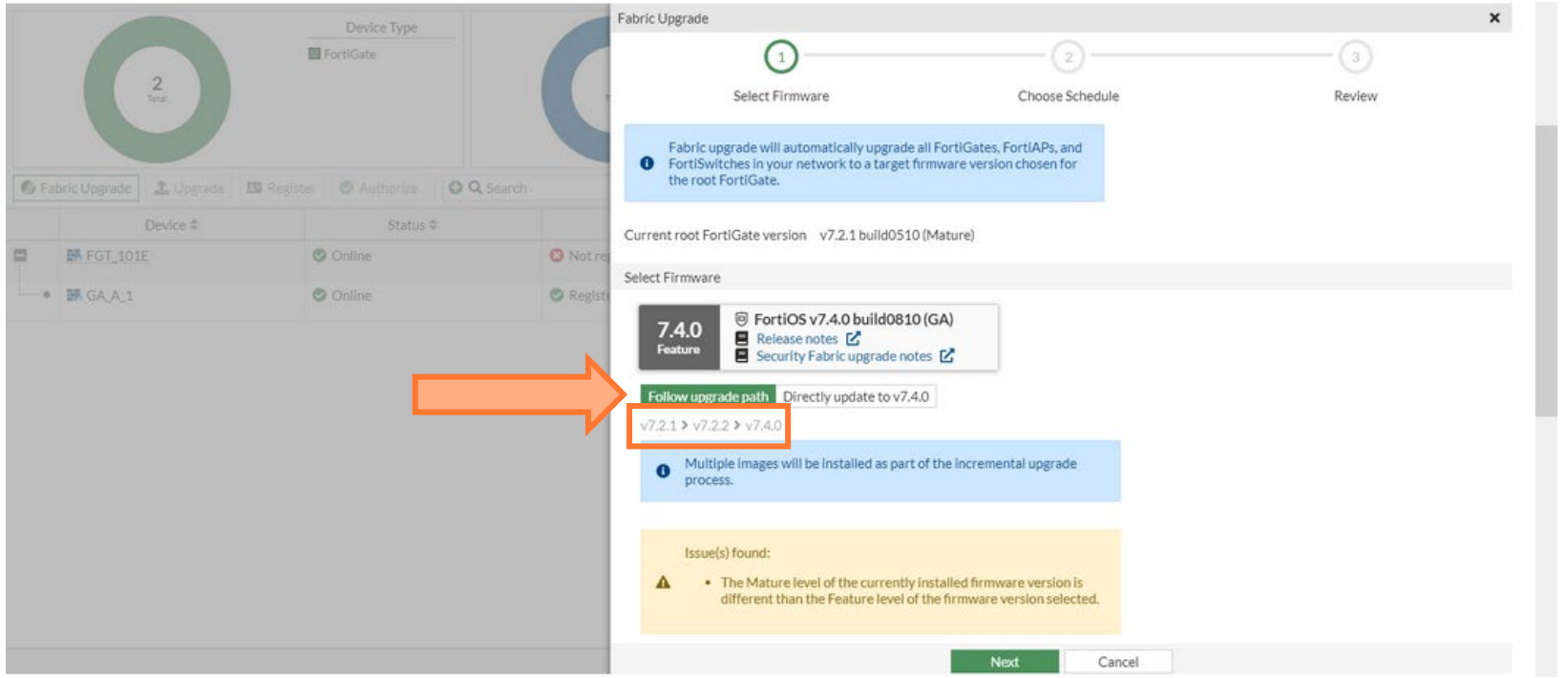


UPGRADE PATH – HOW TO…



1. Navigieren auf ***System → Fabric Management*** und auf ***Fabric Upgrade*** klicken. Der Bereich Fabric Upgrade wird geöffnet
2. Im Abschnitt ***Select Firmware*** die Option All ***Upgrades*** auswählen.

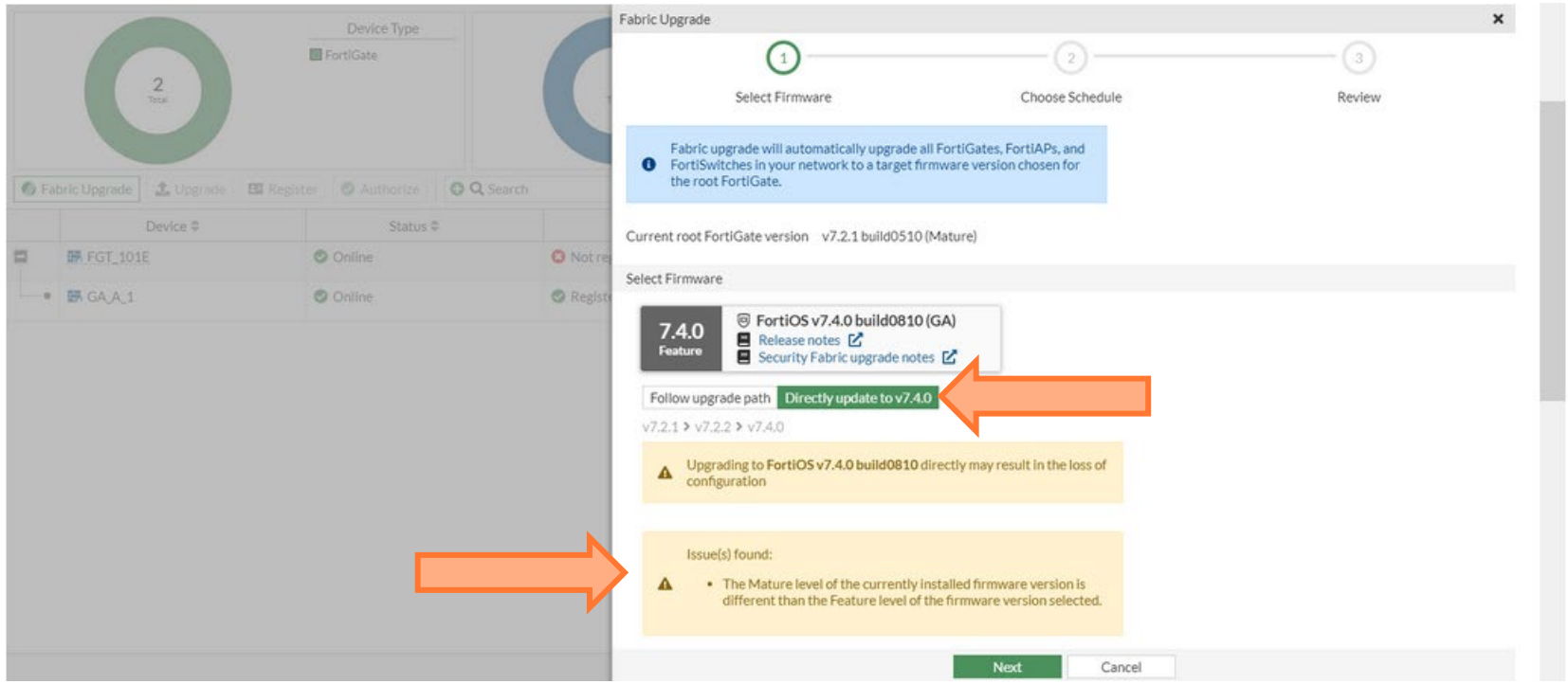
UPGRADE PATH – HOW TO…



3. Die Version ***7.4.0*** auswählen. Nun erscheinen die Upgrade Optionen

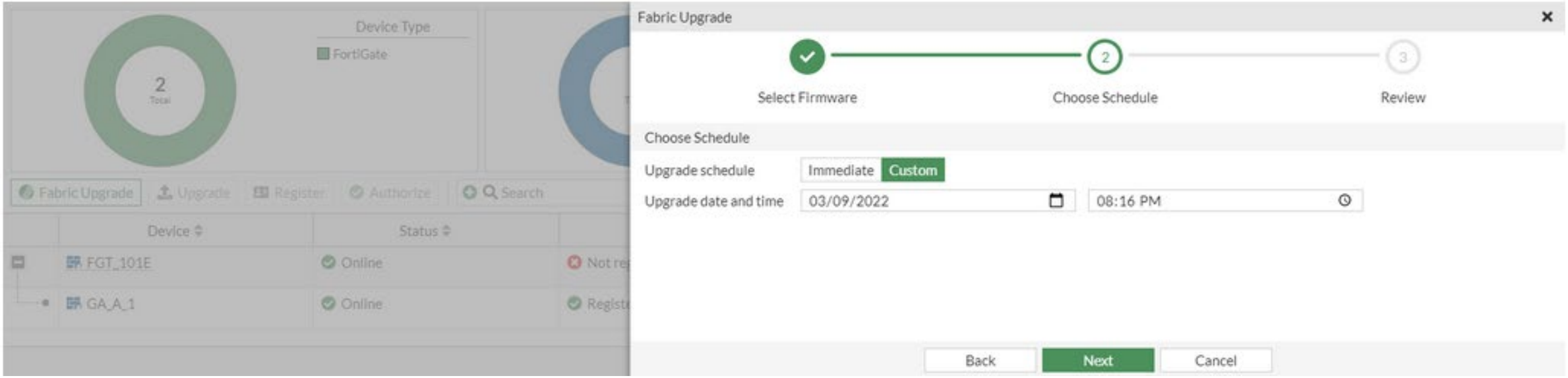
4. Die Option ***Follow upgrade path***. Der Empfohlene Upgradepfad wird angezeigt: ***v7.2.1 > v7.2.2 > v7.4.0***

UPGRADE PATH – HOW TO…



Wenn die ***Directly upgrade to v7.4.0*** gewählt wird, erscheint eine Warnmeldung, dass dies zu einem Verlust der Konfiguration führen kann

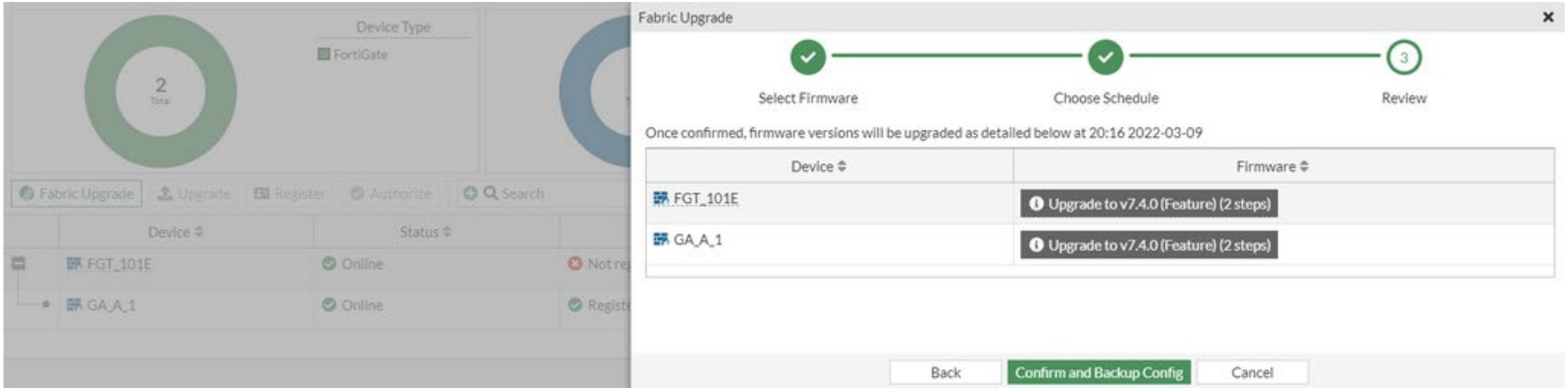
UPGRADE PATH – HOW TO…



5. Mit ***Next*** geht es weiter

6. Wahl des Upgrade-Zeitplan, entweder Sofort oder Benutzerdefiniert. Wenn man "Benutzerdefiniert" verwenden, das Datum und die Zeit für das Upgrade definieren (in diesem Beispiel wird "Benutzerdefiniert" verwendet).

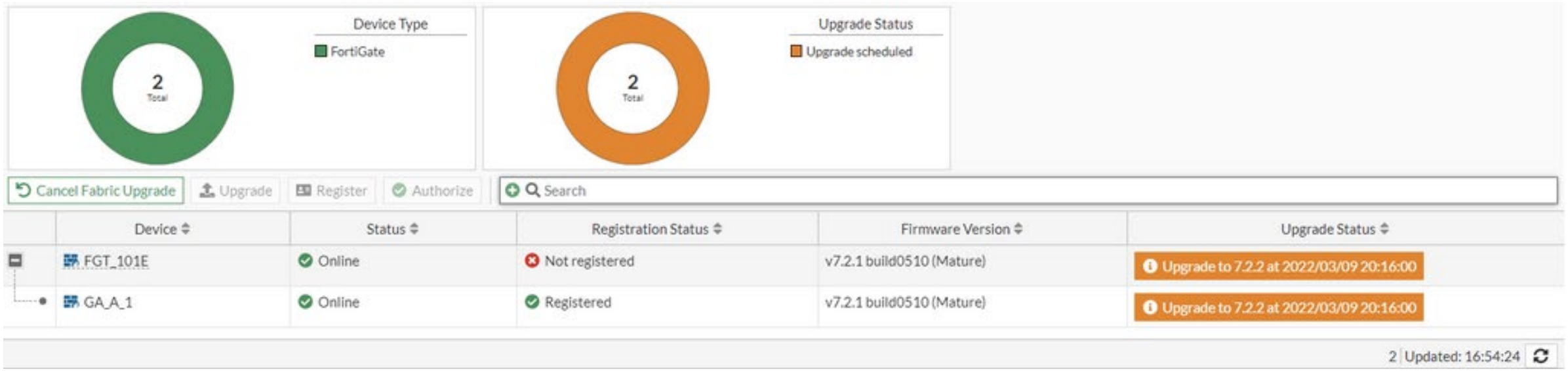
UPGRADE PATH – HOW TO…



7. Nach dem anwählen von **Next** den Zeitplan noch einmal kontrollieren

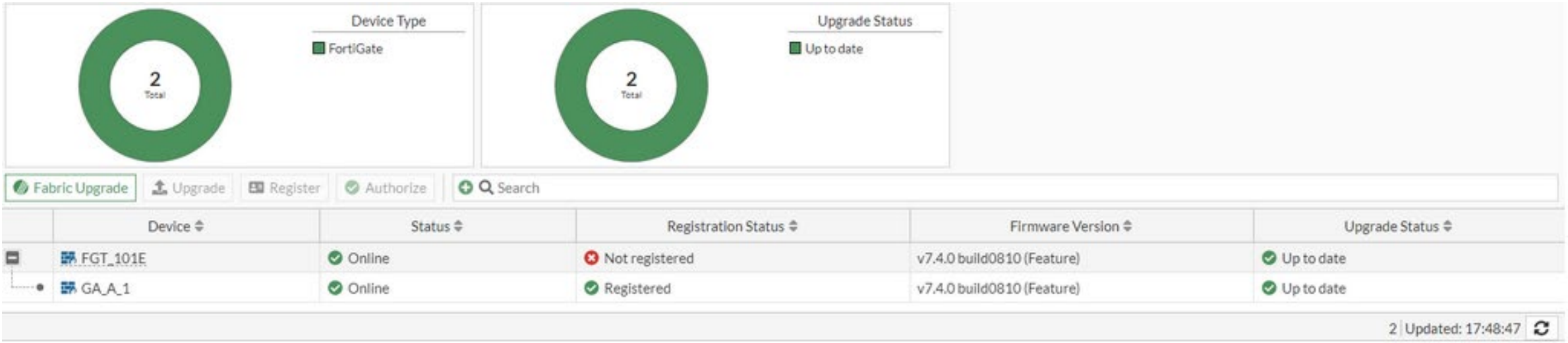
8. Sobald **Confirm and Backup Config** angewählt wird, wird der Upgrade initiert.

UPGRADE PATH – HOW TO…



Der Upgrade-Status für beide FortiGates zeigt an, wann das geplante Upgrade stattfinden wird.
In diesem Beispiel ist das erste Upgrade im Pfad auf Version 7.2.2.
Die FortiGates werden neu gestartet und dann gemäss dem Upgrade-Pfad auf 7.4.0 aktualisiert

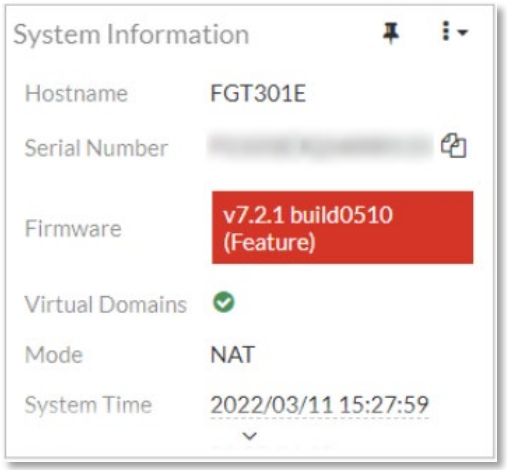
UPGRADE PATH – HOW TO…

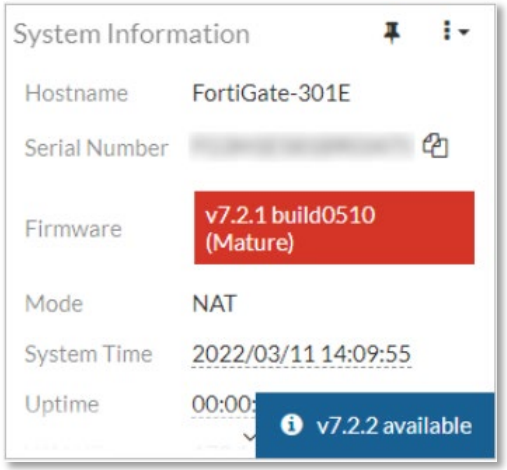


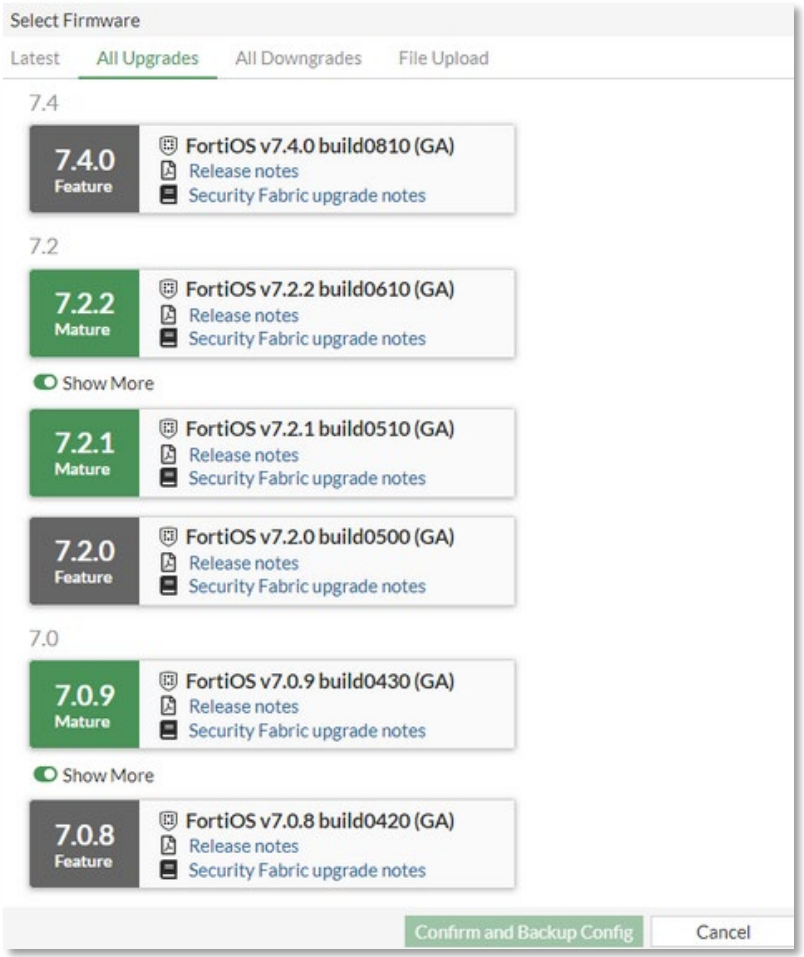
Sobald die Upgrades abgeschlossen sind und auf beiden FortiGates die gewünschte Firmware (7.4.0) läuft, ändert sich der Upgrade-Status in Up to date.

FIRMWARE LEVEL ERSICHTLICH

- **Feature Release:**
  - Neue Features oder CLI Änderungen im Release enthalten.
- **Mature Release:**
  - Keine neuen Features oder CLI Änderungen im Release enthalten

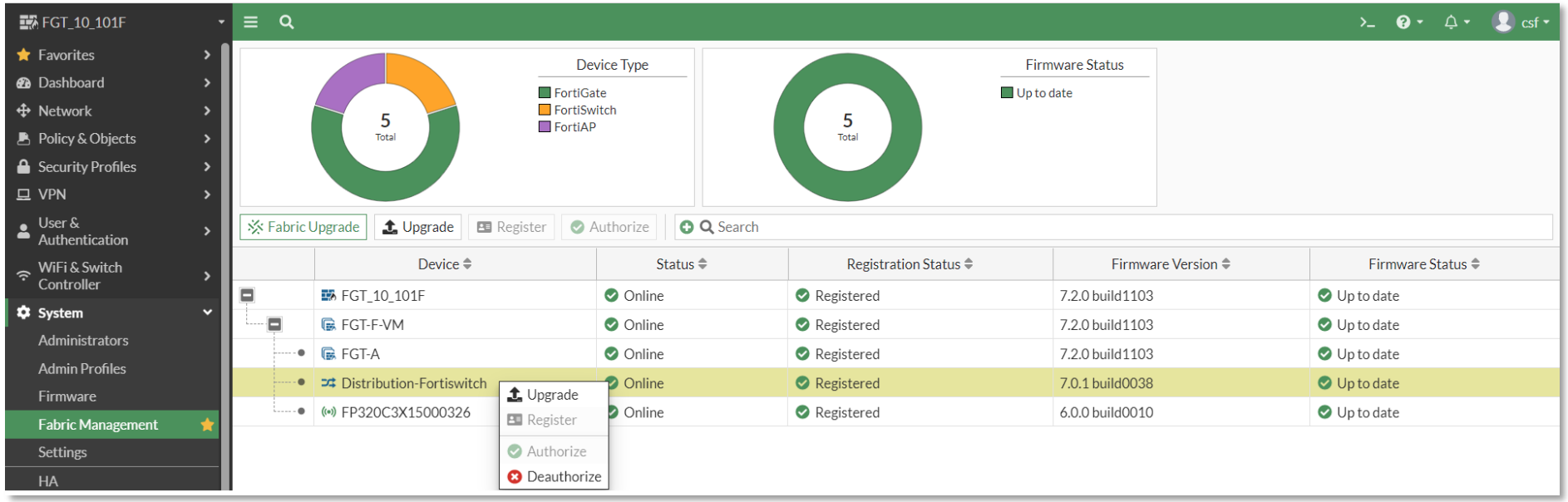






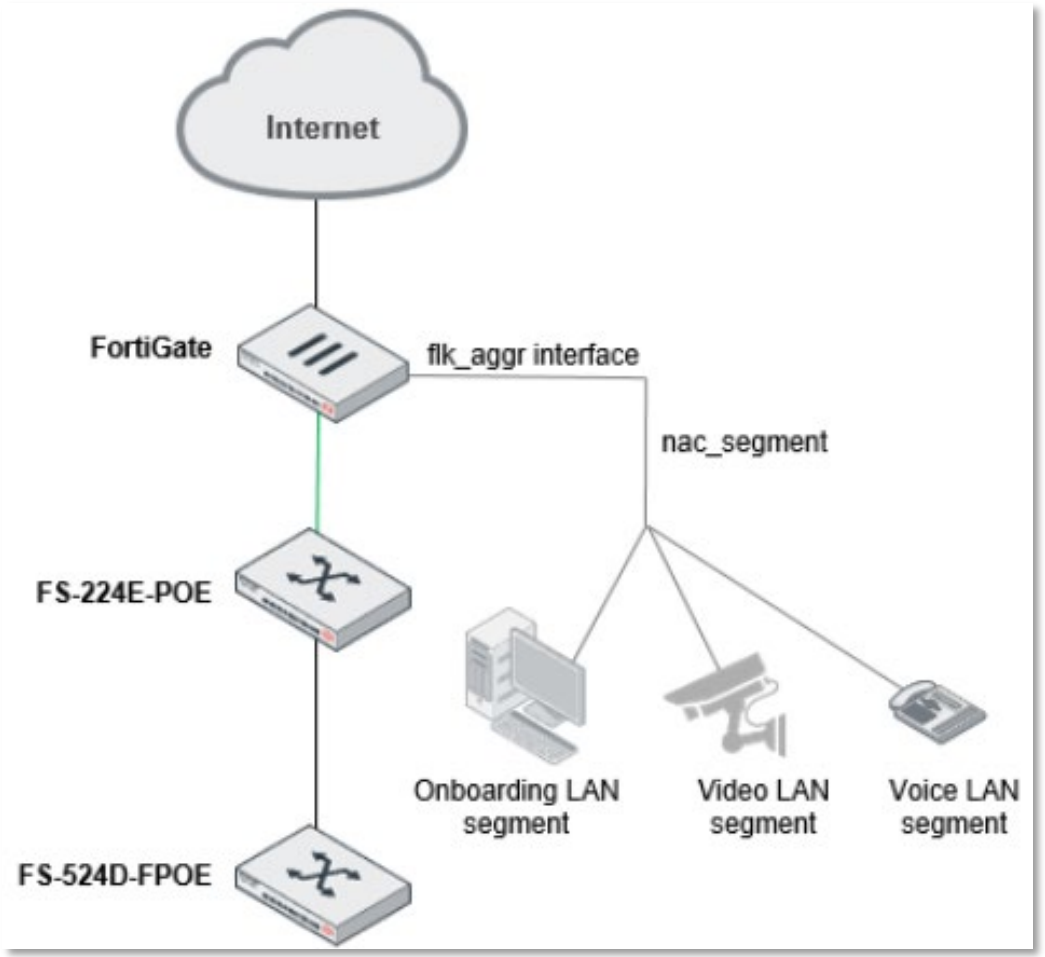
DEVICE MANAGEMENT

- Neue Fabric-Geräteübersichtsseite zur Auflistung von Fabric-Netzwerkgeräten
  - Aufgelistete Geräte - FG, FSW, FAP und FEX
  - Zentralisierte Statusanzeige, Firmware-Verwaltung, FortiCare-Registrierung und -Autorisierung



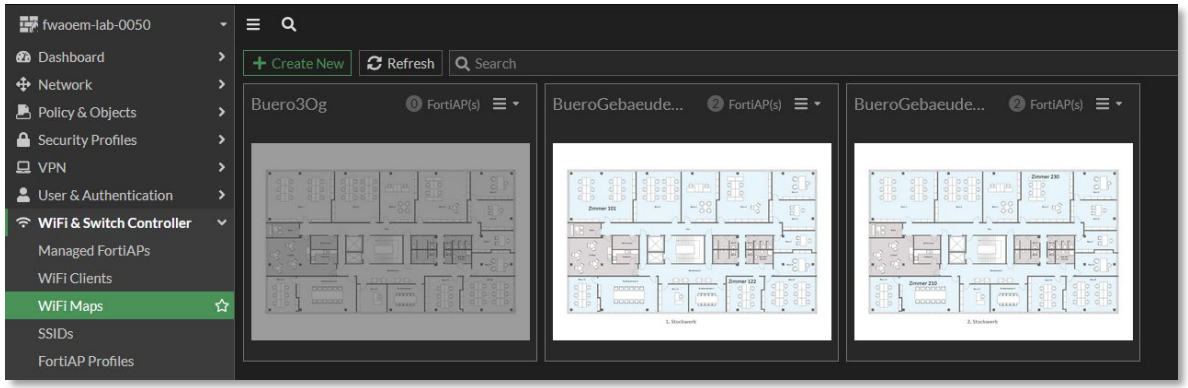
LAN SEGMENTATION GUI

- Hinzufügen von GUI-Konfiguration und Verbesserungen an der NAC-LAN-Segmentierungsfunktion
- Anzeige von NAC-Segment- und LAN-Segment-VLANs als Parent- und Child-VLANs auf der ***Network → Interface*** Seite
- Hinzufügen eines VLAN-Segment-Toggles, um die VLAN-Segmentierung auf einem Switch-VLAN-Interface anzuwenden
- Hinzufügen eines NAC-Einstellungsdialogs zur NAC-Policy Seite, um NAC VLAN zu aktivieren und die primären, Onboarding- und Segment-VLANs zu ändern

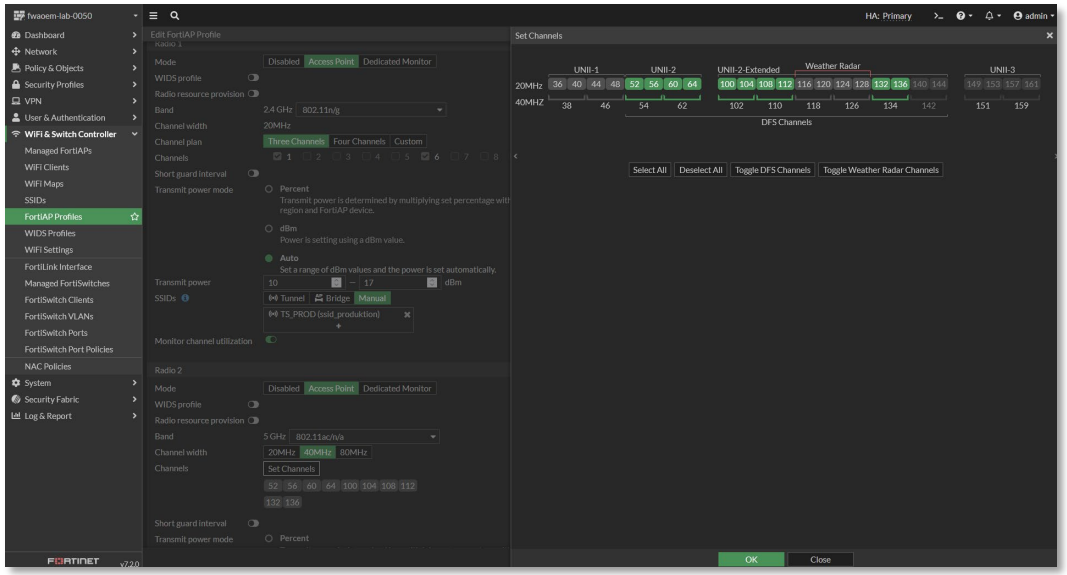


WIFI FEATURES - ZUSAMMENGEFASST

- Mehrere WiFi Karten einlesen:



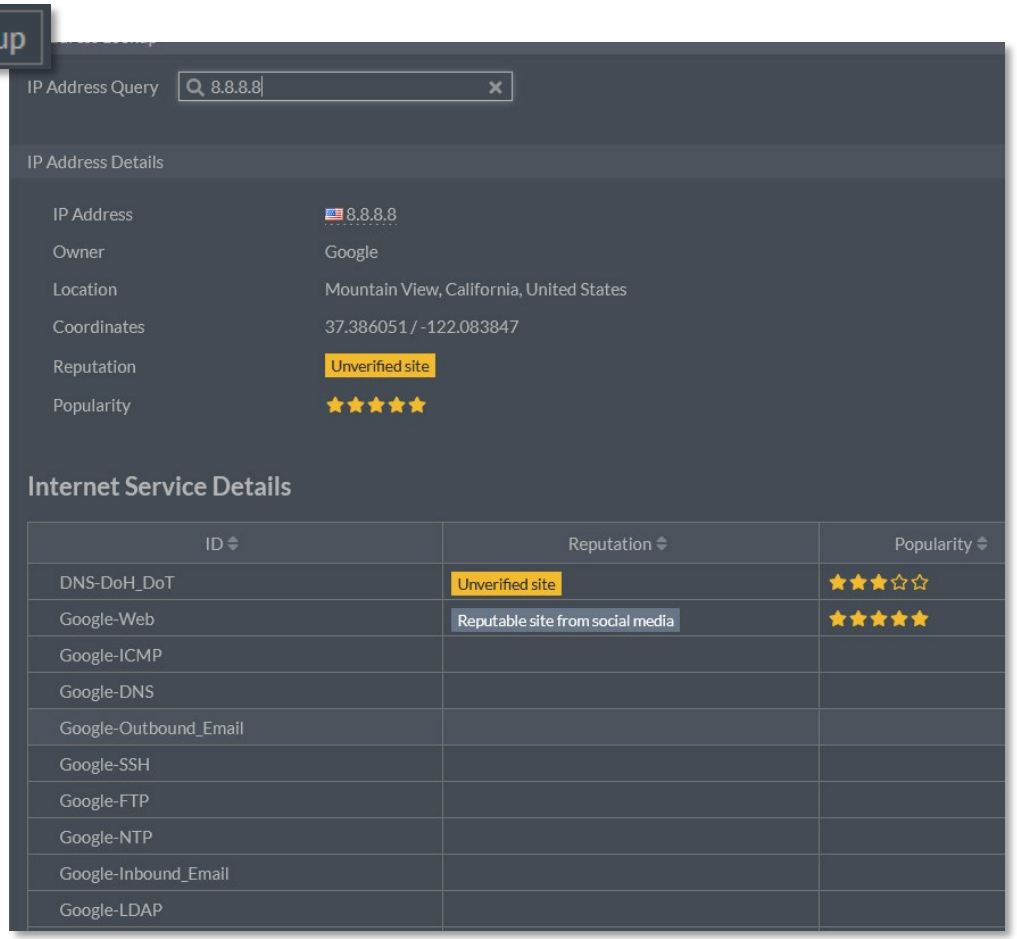
- Verbesserte WiFi-Kanalauswahl im GUI:



Alle Features im Wireless Bereich:
https://docs.fortinet.com/document/fortigate/7.2.0/new-features/937037/wireless

ISDB – IP ADRESSEN LOOKUP

- IP Adressen Lookup in ISDB-Objekten
  - IP-Informationen aus der ISDB und GeoIP Datenbank abrufen
- Die zurückgegebenen IP-Adressinformationen umfassen folgende Angaben:
  - Reverse IP-Adresse
  - Reverse Domain Lookup
  - Standort,
  - Reputation
  - andere Internetdienstinformationen.



https://docs.fortinet.com/document/fortigate/7.2.0/new-features/635185/look-up-ip-address-information-from-the-internet-service-database-page

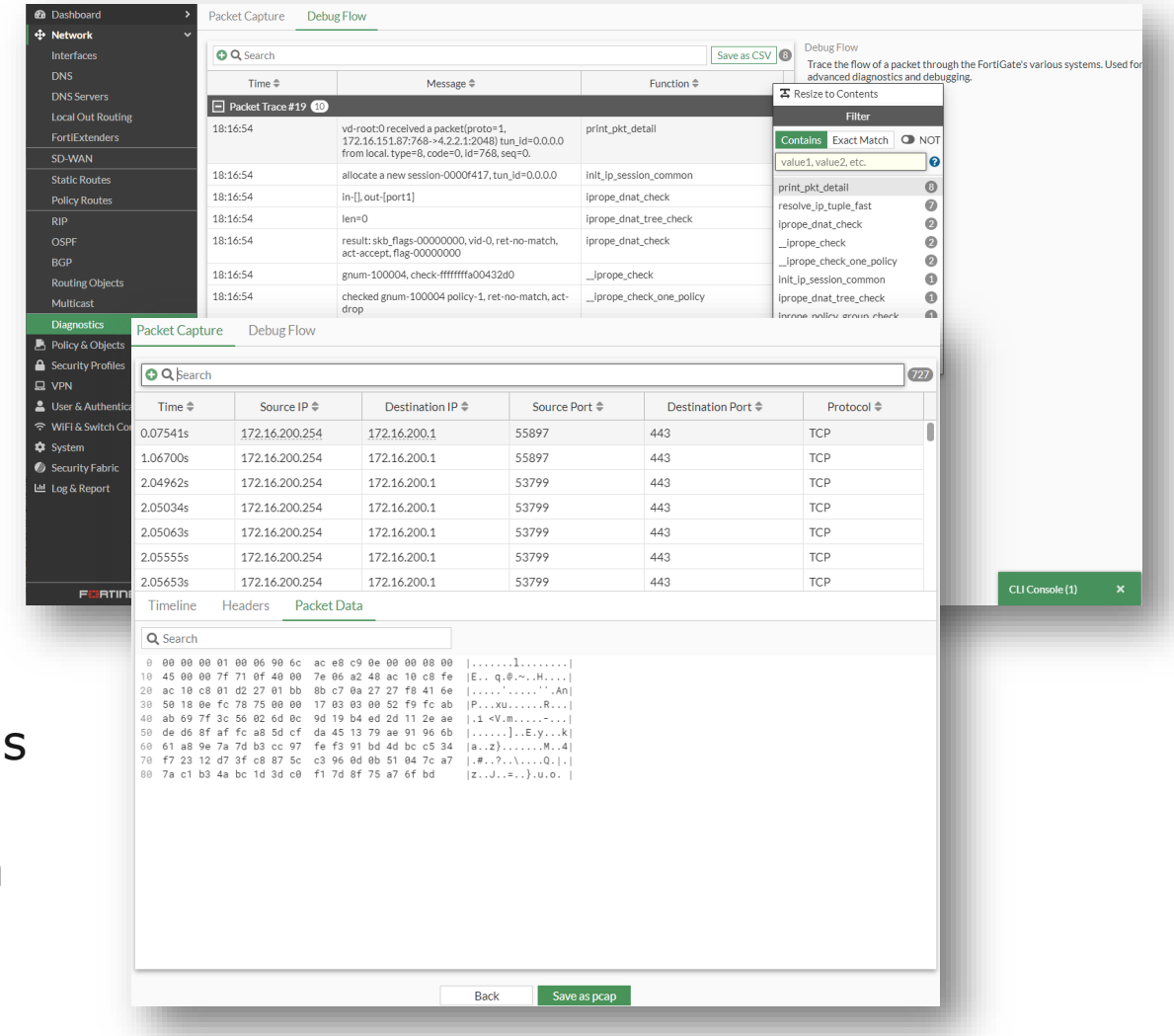
GRAFISCHE DIAGNOSTIK TOOLS

Debug Flow Seite

- GUI-Unterstützung für den Debug-Flow von Paketen
- Tabellarische und Userfreundliche Ausgabe

Eingebaute Echtzeit Paketaufzeichnungs- und Analysewerkzeug

- Paketerfassung kann direkt von dem WebGUI aus untersucht werden
- Beseitigt die Notwendigkeit der Verwendung von Drittanbieter-Viewern wie Wireshark



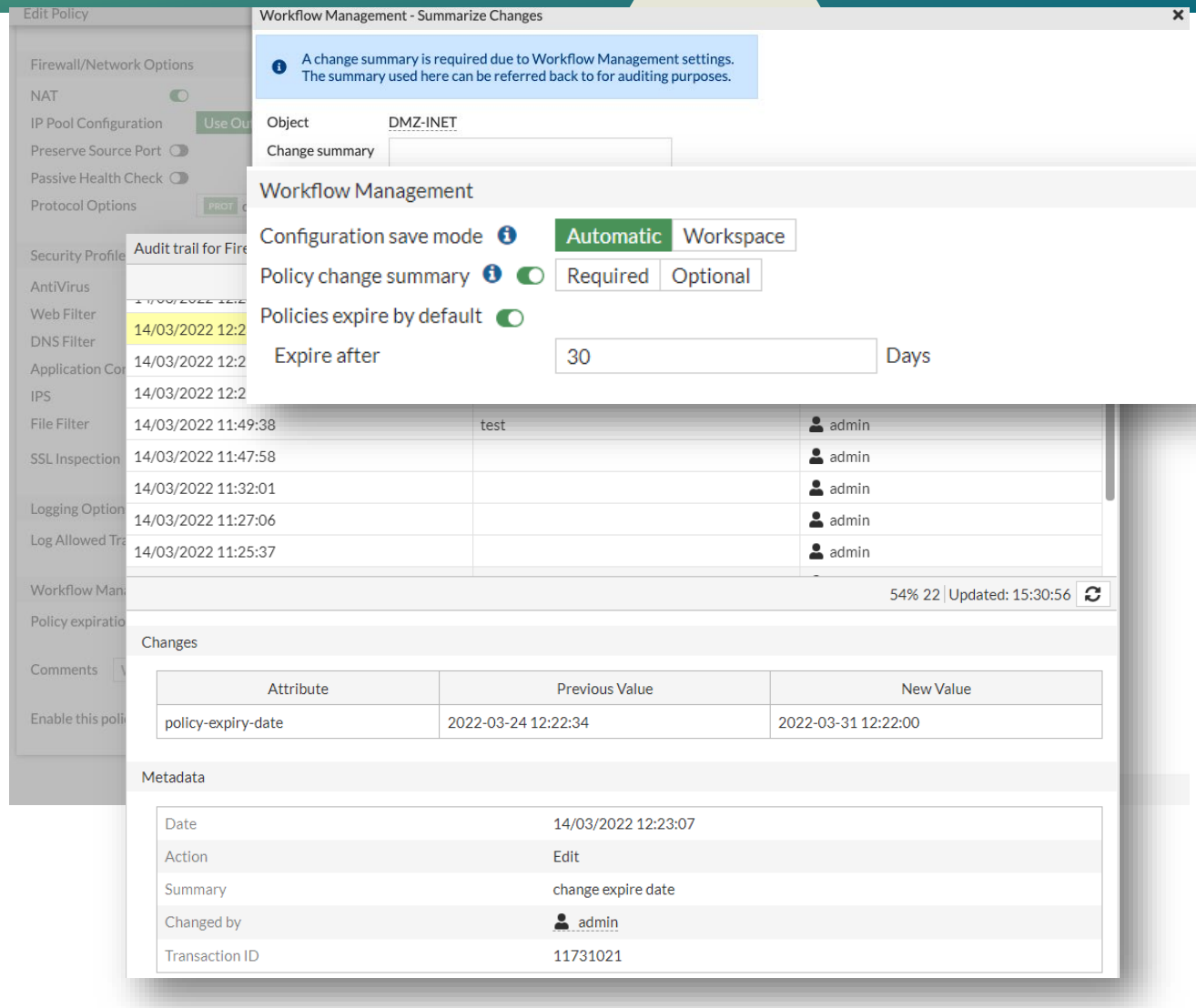
ARTIKEL DIAGNOSE FEATURES / ISDB LOOKUP

- Debug Flow
  - https://docs.fortinet.com/document/fortigate/7.2.0/new-features/462154/embed-real-time-packet-capture-and-analysis-tool-on-diagnostics-page
  - https://docs.fortinet.com/document/fortigate/7.2.0/new-features/38044/embed-real-time-debug-flow-tool-on-diagnostics-page
- Paket Capture/Sniffer:
  - https://community.fortinet.com/t5/FortiGate/Technical-Tip-Debug-flow-tool/ta-p/213238
  - https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-run-a-real-time-Wireshark-capture-on/ta-p/213805
- ISDB Lookup
  - https://docs.fortinet.com/document/fortigate/7.2.0/new-features/635185/look-up-ip-address-information-from-the-internet-service-database-page

WORKFLOW MANAGEMENT

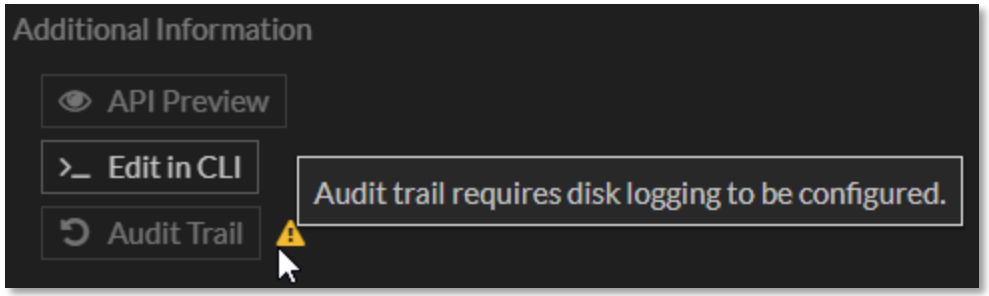
Policy Change Summary

- Zusammenfassung von Policy Änderungen
- Bei Policy Änderungen erscheint ein Comment-Feld für den Administrator zur Eingabe von etwaigen Kommentaren.
- Optionen wie "immer erforderlich" und "optional"
- Admin kann Audit Trail für eine Firewall-Regel anzeigen

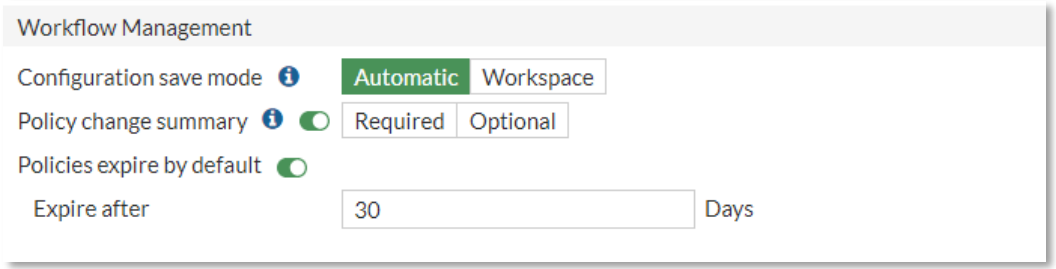


WORKFLOW MANAGEMENT

- Policy Change Dokumentation
  - Kommentar bei jeder Firewall-Regel
  - Änderung kann Optional oder Erzwungen werden
  - Um die Audit Logs zu sehen ist eine Disk notwendig

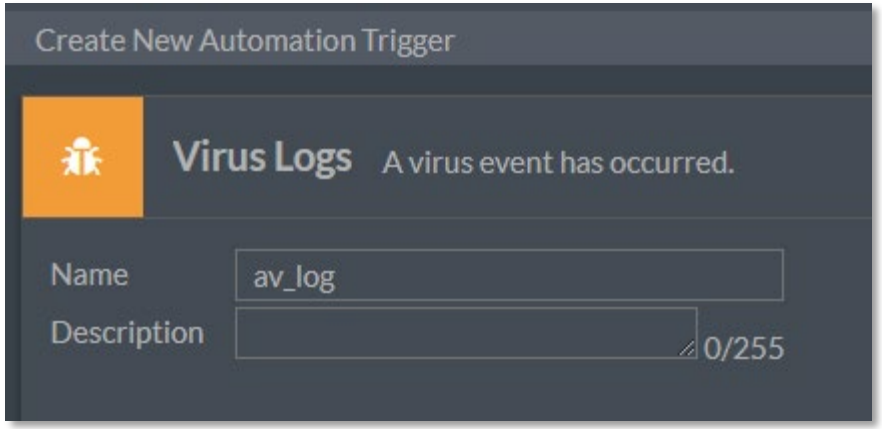


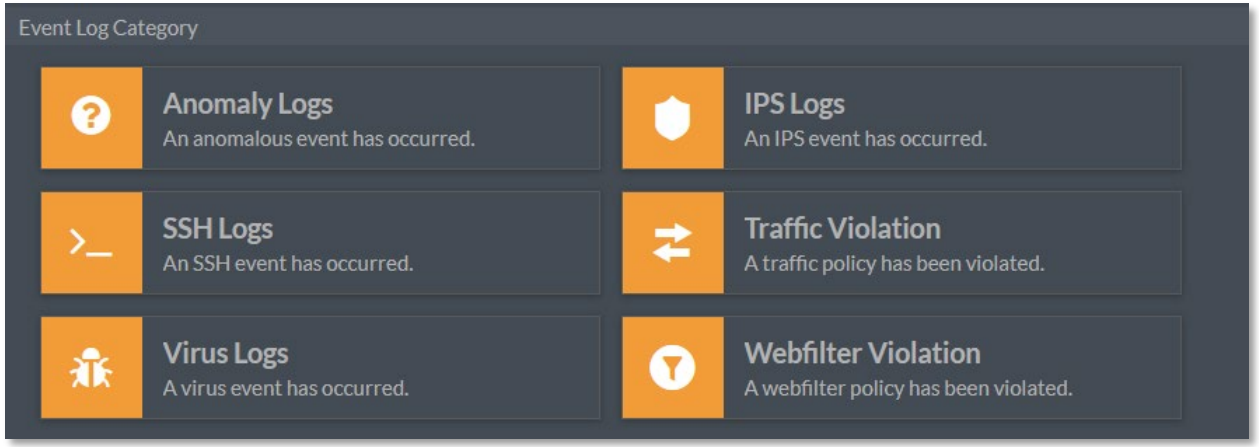
- Gültigkeit der Firewall Regeln
  - Wenn diese Funktion für eine Firewall Regel aktiviert wird, kann der Administrator den Zeitpunkt für das Auslaufen der Policy definieren(default Wert ist 30 Tage)
  - Der Wert kann selber definiert werden.



SECURITY FABRIC | AUTOMATION STITCHES

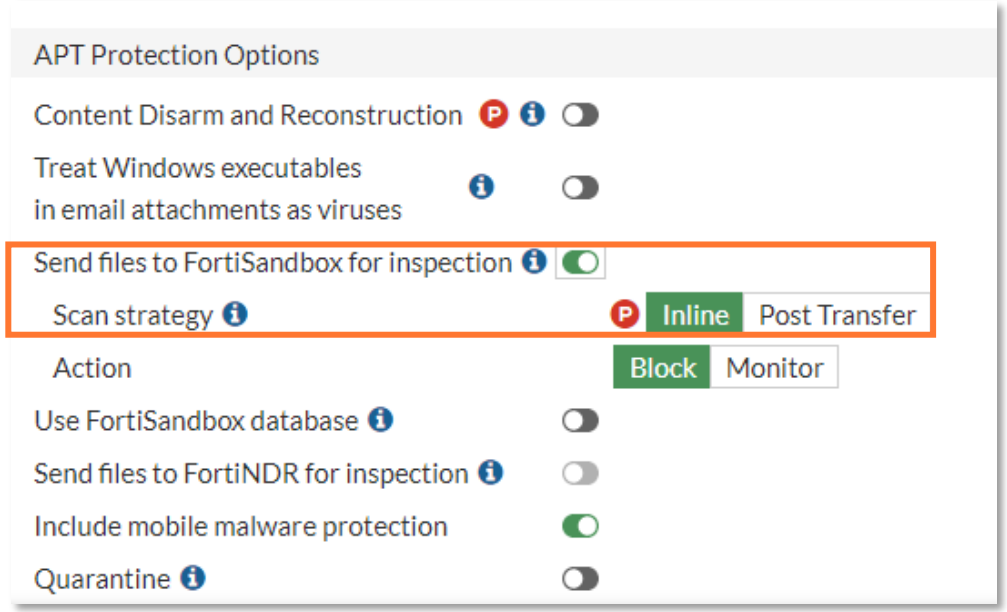
- Neue Automation Trigger
- Es wurden sechs neue Trigger hinzugefügt, welche auf verschiedenen **Eventlog Kategorien** basieren:
  - **Anomaly Logs**
  - **SSH Logs**
  - **Virus Logs**
  - **IPS Logs**
  - **Traffic Violation**
  - **Webfilter Violation**

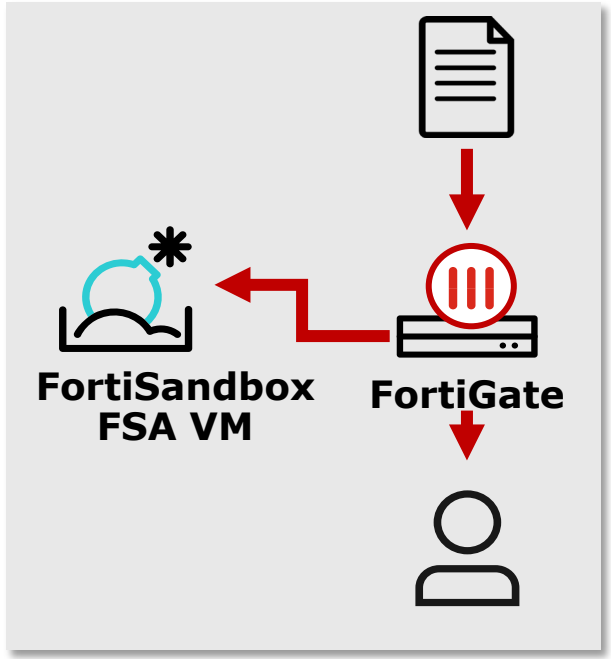




FORTISANDBOX INLINE SCANNING

- Unterstützung von Hold-&-Release für von FortiSandbox untersuchte Dateien
  - FGT kann so konfiguriert werden, dass es auf das FSA-Ergebnis wartet, bevor die Datei an das Ziel freigegeben wird.
  - Administratoren können künstlich erzeugte Verzögerung konfigurieren, um das teilweise oder endgültige, bekannte Ergebnis der FSA abzuwarten
- Verwendet HTTP2 (Streaming), damit die FGT den Download sowohl an die FSA als auch an den Endbenutzer weiterleitet und nur die letzten Pakete zurückhält





KONFIGURATION ÜBER DIE CLI

- FortiSandbox inline scanning aktivieren:

```
config system fortisandbox
    set status enable
    set inline-scan {enable | disable}
    set server <fortisandbox_server_ip>
end
```

- Konfiguration FortiSandbox scanning Optionen im Antivirus Profil:

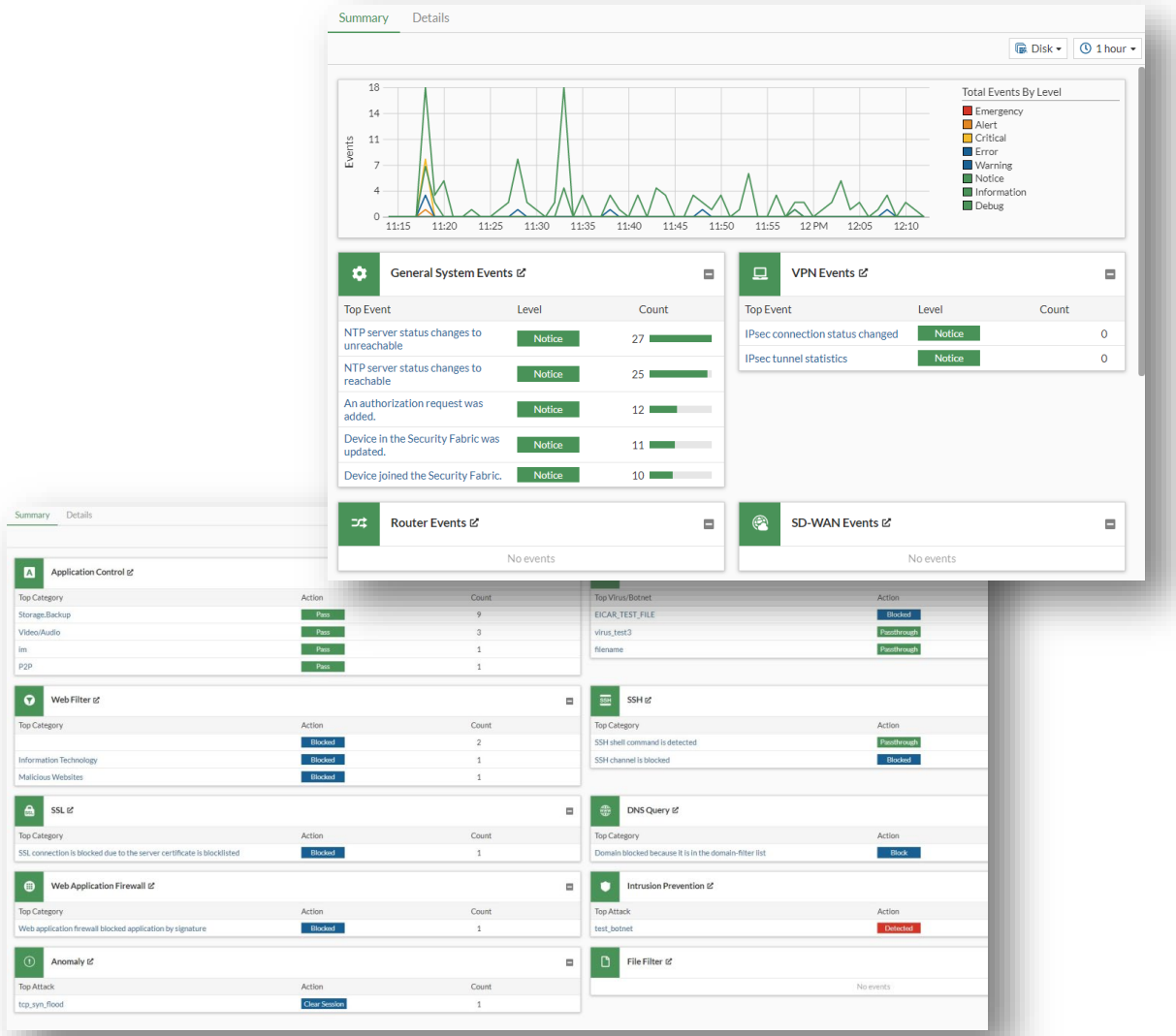
```
config antivirus profile
    edit <name>
        set fortisandbox-mode {inline | analytics-suspicious | analytics-everything}
        set fortisandbox-error-action {ignore | log-only | block}
        set fortisandbox-timeout-action {ignore | log-only | block}
        set fortisandbox-max-upload <integer>
        config {http | ftp | imap | pop3 | smtp | mapi | cifs | ssh}
            set av-scan {disable | block | monitor}
            set fortisandbox {disable | block | monitor}
        end
    next
end
```

https://docs.fortinet.com/document/fortigate/7.2.0/new-features/571153/fortisandbox-inline-scanning

ÜBERARBEITETE LOG SEITEN – SYSTEM EVENTS

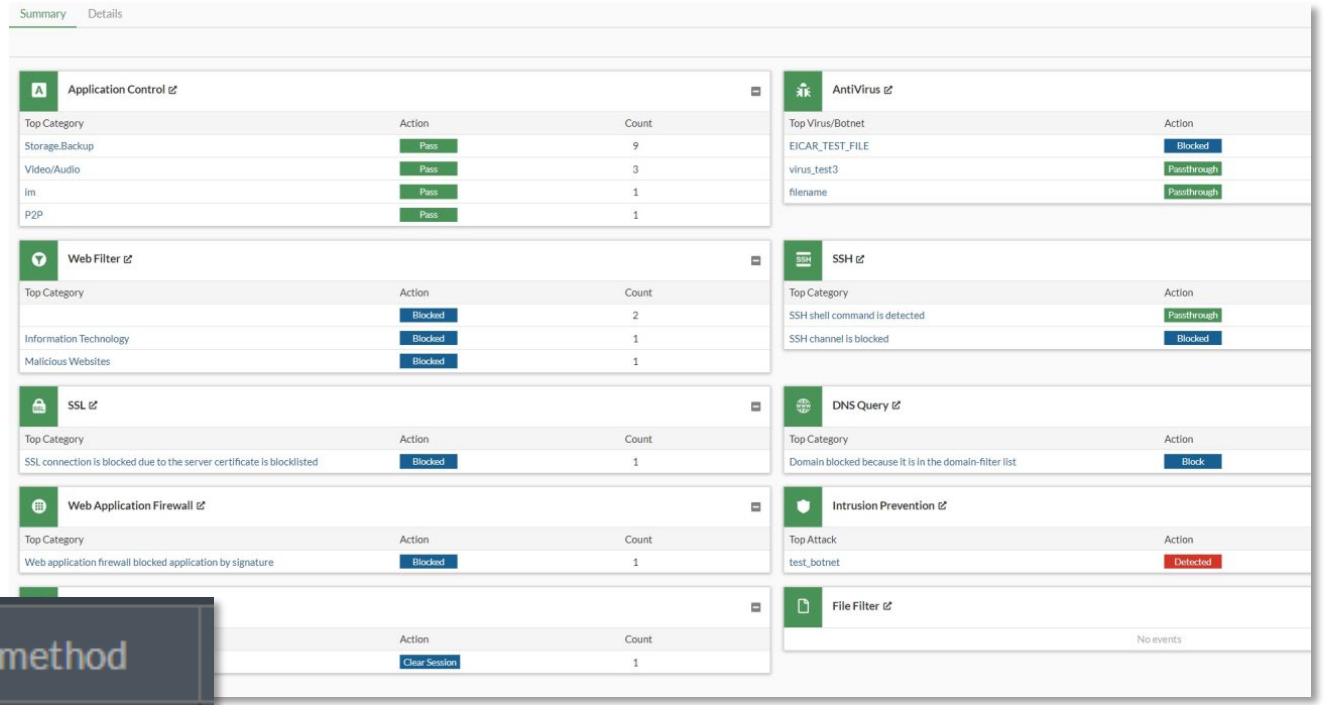
- System Event Log Seite
  - Enthält eine neue Registerkarte "Zusammenfassung
  - Durch Anklicken eines Ereignisses auf der Registerkarte "Zusammenfassung" gelangt der Benutzer automatisch zur Registerkarte "Details" mit den entsprechenden Filtern

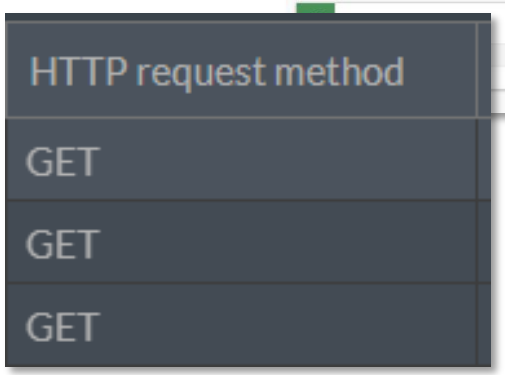
- Security Log Seite
  - UTM-Protokoll-Subtypen sind jetzt kombiniert
  - Zugang zu interessierenden Logs über die neue Zusammenfassungsseite



ÜBERARBEITETE LOG SEITEN – SECURITY LOG

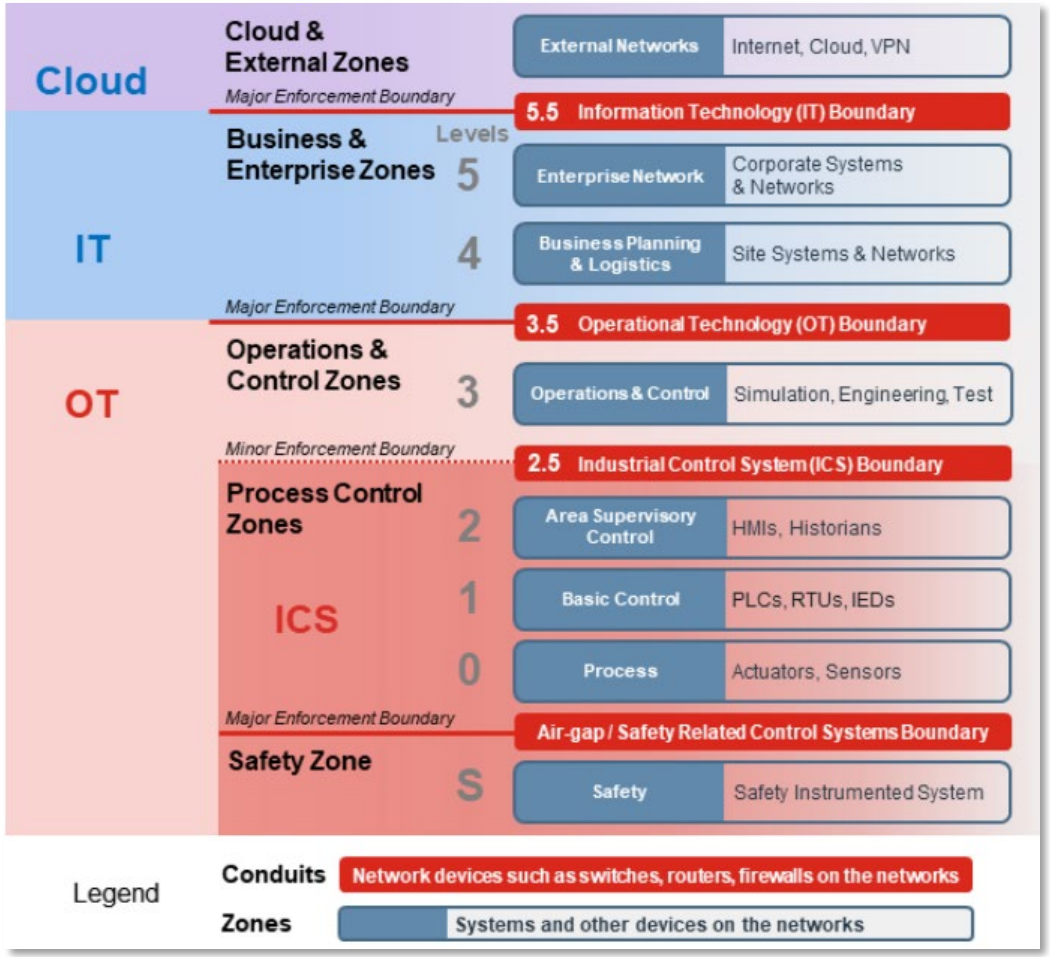
- Security Log Seite
  - UTM-Protokoll-Subtypen sind jetzt kombiniert
  - Zugang zu interessierenden Logs über die neue Zusammenfassungsseite
- HTTP Transaction Log Feld überarbeitet
  - HTTP Method Feld wurde hinzugefügt
  - Agent wurde hinzugefügt
  - Referenz URL wurde hinzugefügt





OT ASSET VISIBILITY

- Voraussetzung: IoT detection service subscription
- Grafische Übersicht der OT/IoT Devices
- Devices lassen sich via drag'n drop in die verschiedenen Purdue Level ziehen



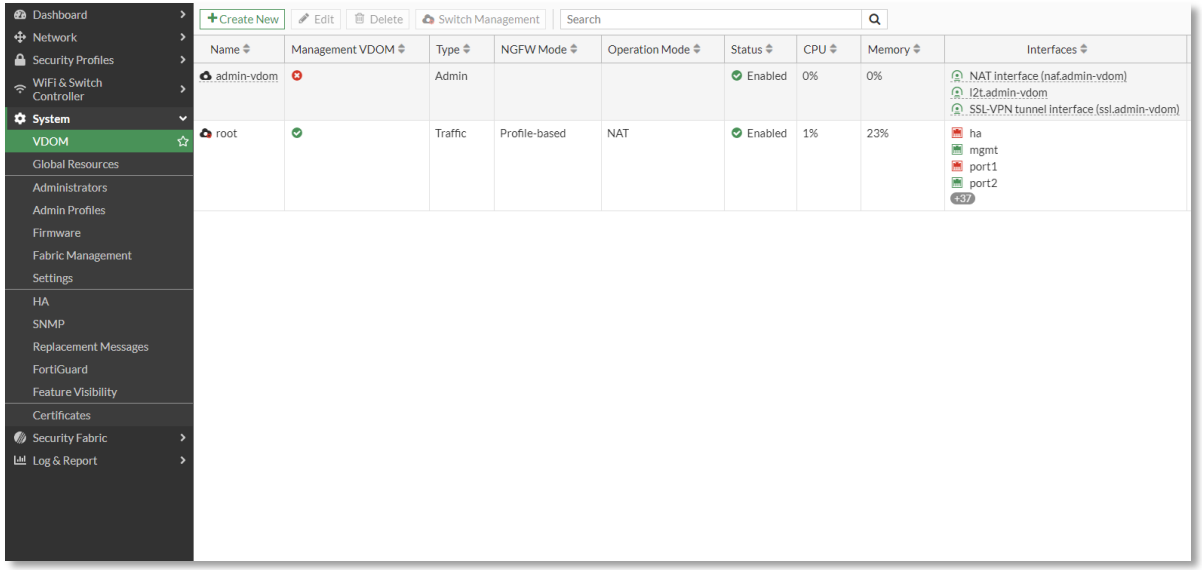
- Purdue Enterprise Reference Architecture ist ein Referenzmodell für Unternehmensarchitektur aus den 1990er Jahren, das von Theodore J. Williams und Mitgliedern des Industry-Purdue University Consortium for Computer Integrated Manufacturing entwickelt wurde. Wikipedia (Englisch)

https://docs.fortinet.com/document/fortigate/7.2.0/new-features/498242/add-ot-asset-visibility-and-network-topology-to-asset-identity-center-page

DEMO OT VIEW

VDOM - TYPEN

- Organisieren von VDOMs für bestimmte Zwecke
  - 2 VDOM-Typen = Traffic, Admin(Management)
  - Admin-VDOM ersetzt den Spilt-Task-VDOM-Modus

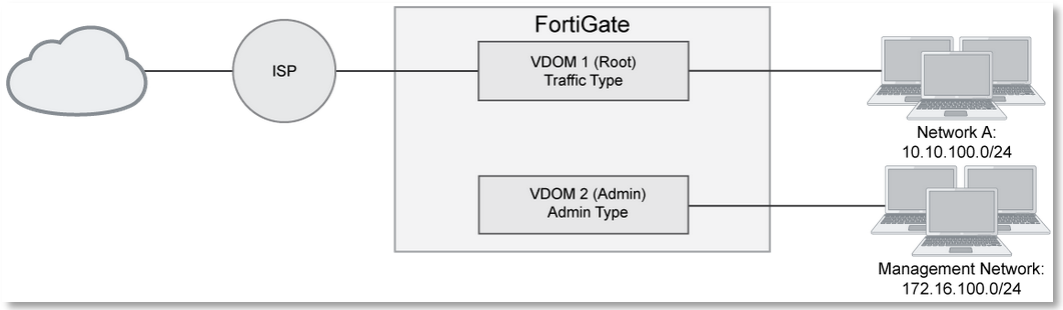


- VDOM Mode aktivieren:

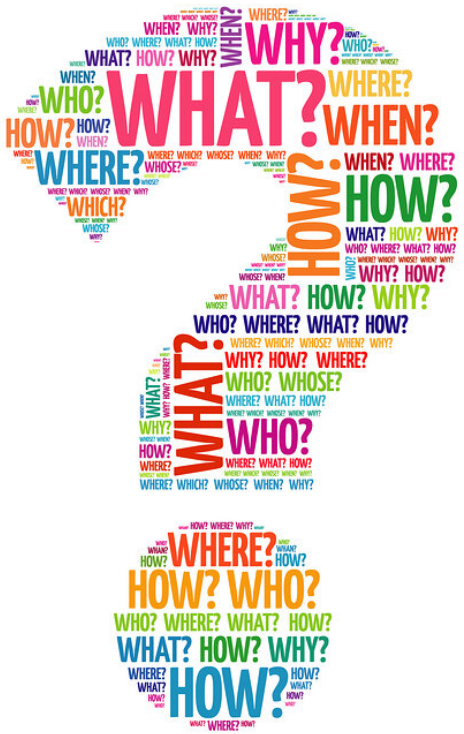
```
config system global
     set vdom-mode multi-vdom
end
```

- VDOM Typ definieren:

```
config system settings
    set vdom-type {traffic | admin}
end
```



Q&A



Gerne stehen wir euch nun für Fragen und Anregungen zur Verfügung.
Fragen gerne an fortinet-ch@also.com
Besucht auch https://fortinet.also.ch/wiki

THANK YOU